CAS / DRM Reality Check

-

How to Think Like a Criminal, Avoid Crypto FUD and Follow the Rest of the World

Robin Wilson

Nagra

Crime & Business Models 101

- Commercial pirates are very smart
- Thorough business planning including:
  - Cost of developing/sourcing and selling “products”
  - Threats
  - Rewards
- Successful pirate business models have high rewards and low threats
- “Costs” include computational costs
  - Server / Cloud hosting, Bandwidth, Billing Systems, Credit Card Fulfillment Fees

Market Research used by the Dark Side V1

	Ease to Copy	Ethical?	Raw Margin	Margin After Mass Use	Risk
Paper Money	Medium	Barely	Medium / High	Medium	Very High = Secret Service
Gold	Impossible without Alchemy?	Victimless Crime so Yes	-	-	Thermo Nuclear Meltdown
DVD's	Easy	Charitable Act	High	Low	Low
Hollywood UHD Content	**Medium / Hard**	**In the Constitution?**	Infinite	**High**	**Low**

Market Research used by the Dark Side – ReSecured

After Technical improvements and educational efforts on “Ethics”

	Ease to Copy	Ethical?	Raw Margin	Margin After Mass Use	Risk
Paper Money	Medium	Barely	Medium / High	Medium	Very High = Secret Service
Gold	Impossible without Alchemy?	Victimless Crime so Yes	-	-	Thermo Nuclear Meltdown
DVD’s	Easy	Charitable Act	High	Low	Low
Hollywood UHD Content	**Very Hard**	**Clearly Illegal AND Antisocial**	Infinite	**Low or Zero**	**High**

Categories of Media Hackers

Group / Characteristic	Final User	"Tekkie"	Hacker	Professional Pirate
End-user profile	No technical skills	Engineer with limited means	Sophisticated Engineer with limited means	Sophisticated Engineer w / unlimited means
Time willing to spend on "pirate device"	Little to none (consumer-behavior)	Limited (an afternoon)	Hobbyist, up to several hours each day	Limited only by profitability of time spent
Perennity Required	Long (yearly)	Moderate (1-2 mos) depends on effort	1 day	Depends on effort required
Cost	Less than subscription fee ($200)	Very low	Moderate (could be 100s-1000s of dollars)	Millions of dollars, limited to profitability
Friendliness of "pirate device"	User friendly	Moderately friendly	Moderately friendly-unfriendly	N / A
Ease of use (of pirate device)	Very easy	Somewhat easy	Somewhat easy to moderately inconvenient	N / A
Aesthetics of device	Obtrusive Must be unobtrusive	Unobtrusive to mildy cumbersome	Obtrustive	N / A

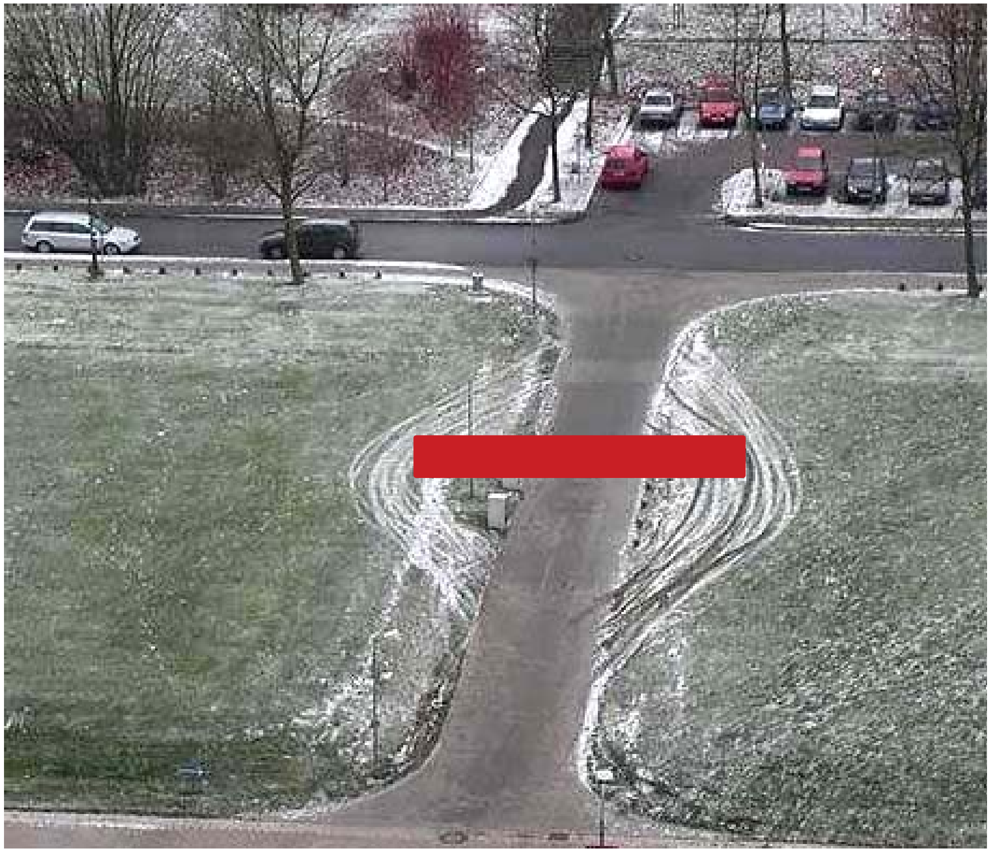
Merdan's Attack Levels	Simple Manipulation	Casual Hacking	Sophisticated Hacking	University Challenge	Criminal Enterprise

Breaking the Evil Business Plan

- Understand your enemy - Reverse engineer his business plan and break it!.....
- Don’t forget magic downloadable replaceable solutions might work better for your enemy
- Don’t get sidetracked into potentially irrelevant crypto discussions like key length

Key Length – *Almost* Irrelevant

- AES 128 sensibly prescribed by MovieLabs
- Guessing a long key is extremely hard and expensive
- Irrelevant to hacker
- Irrelevant to security

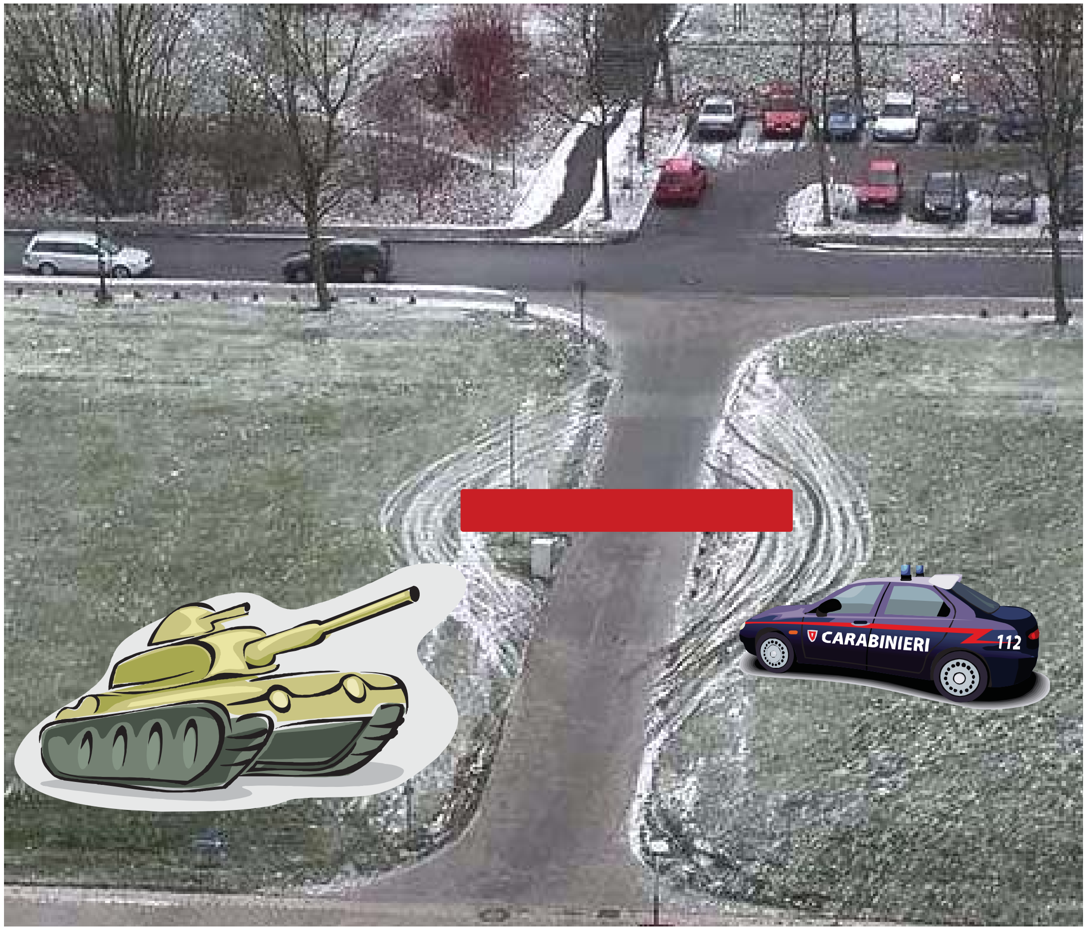


Hardware vs. Software Security

- Beware Idyllic generalizations
- “Software Only” is often a bogus discussion
  - Hardware (CPU) runs Software!
  - Software runs on Hardware (CPU)!
- The important issue is whether the CPU *and* Software environment is secure
- A CPU can be secure or insecure
  - Unless otherwise defined a generic CPU is Insecure
  - HW Root of Trust required for high value content must have Secure Environment

Enforcement Works

- □ Local enforcement
  - ○ Criminalizing…
- □ Global enforcement
  - ○ Customs, IP Theft…
- □ Breaks business plan
- □ Raises costs and risks



Content Owner Considerations

- Content owners (Studios) have a long and sometimes painful history of piracy
  - Technical, legal and business groups to combat piracy
  - Some of their requirements are defined in the MovieLabs Specification Enhanced Content Protection
- Content Security companies (CAS, DRM) negotiate, interpret, implement these requirements
  - MVPD requirements are most often driven by Studio requirements
- Beware of telling Studios how to do their job
  - Been there, done that, not fun (and Nagra has 20+ years & several $Billion of R&D investment)

Threat Models and Misplaced Analogies - I

- A Commercial hacker is clever – goes after the easiest & safest path to profitability
  - Example:
    - Conus DBS MVPD has 400M homes passed and MUST use same keys
    - Cable MVPD may have 40M home passed max and may segment keys
    - Hacker focuses entirely on DBS, ignores Cable
  - Do not directly infer any security technology conclusion from this!
  - Likewise technologies with small and/or low ARPU deployments that are not hacked means hackers are not stupid

Threat Models and Misplaced Analogies - II

- Security that works for years in banking or credit cards must be secure for video?
  - Wrong!
  - Banking transaction are in currency. Currency is unique and tied to a specific person that often cares very much at even 1c rounding errors. Authorities jump on this type of crime.
  - MVPD transactions are in media streams. Few / zero people notice if it gets copied. Even less care. Worse, the authorities often don’t care.
- Threat models aren't even just about the threat of hacking but are about the threat and consequences of the hacking.

The Myth that Downloading Cures All

- Not only must we secure the HW platform for Downloadable “SW Only” Security but the “Downloader”
- The Downloader (and associated authentication processes) are directly responsible for ensuring the download is “safe” or secure.
- What if hacker find bugs in the downloader (I can almost guarantee they will)?
    - We download a new downloader?
    - We need a downloader for the downloader to do that?
    - What if that becomes compromised…. a third downloader??
- Sure, a well defined chain of trust is required but that is the very function that gets compromised by bugs

CAS, DRM and Dis-aggregation

- CAS and DRM always protects the Audio and Video payload and associate output controls
- Some data embedded in video so protected by default
- Associated meta-data (guide, extended guide, captions etc) may or may not be protected by CAS or DRM
- Data service may be protected by other means outside scope of CAS / DRM such as well known client server authentication schemes
- Processing overhead for meta-data MAY have performance impact on CAS or DRM client

Beware of Undisclosed Secrets & Bogus Standards

- Scrambler standards that are not standards
  - Missing information like IV (Initialization Vector)
  - A fixed non-copyrightable, non-patentable 56 bit number with no security value
- Keyladders such as SCTE 201 Profile 0 (ETSI TS 103 162)
  - “However, use of ETSI TS 103 162, described below as Profile 0, is discouraged as it allows use of undisclosed algorithms and therefore undisclosed and unknown intellectual property. This standard specifies certain processes which are both necessary for interoperability and not specified in the ETSI standard.”
- Scramblers, Keyladders, Root of trusts etc should be FRAND or Free and TOTALLY disclosed

Diversity Helps

- Avoiding hack one, hack all a very high priority in security
  - Many ways to achieve this
  - Unique device keys not enough
  - Diversifying SW an option
  - Diversifying HW an option
    - Secure operating environments come in many flavors of design and robustness, thus offering some diversity
    - A single HW roof of trust undermines diversity and may become the critical flaw
    - A single HW root of trust may constrain innovation

Positive Developments

- Key sharing / simulcrypt now proliferates
  - DRM deployment showing the way - Now used in multiple DRM systems including MPEG DASH, Netflix
  - Avoids head-end – CAS – CE/STB lock-in
  - Verizon successfully forced cooperation
  - Now Charter
  - So can others?
- All SoC (System on a chip) suppliers now have a range of secure media processors / execution environments
  - Enables SW downloads into a robust secure environment
- Choice of free fully disclosed scramblers available along with secure processing environments and SW tools

Conclusions

- Secure trusted execution environments, free open scramblers and SW tools are now widely available allowing innovation and new entrants
- Key-sharing, (or simulcrypt, or Simulcrypt) works for OTT providers and the rest of the world
- Avoid bogus standards and vendor lock-in – Verizon can do it, perhaps now Charter, so why can’t others?
- For total interoperability and long term survivability the downloading and recovery functions will need more focus and perhaps options